REMARKS

Reconsideration of this application and allowance of the claims, as amended, is respectfully requested.

The amendments to the claims 2, 3, 5, 6 and 19 are in response to the objections to the claims as raised on page 2 of the Office Action. Also, the newly added claims 27-29 are supported at page 7, lines 13-16 of the specification. Claim 30 is supported by original claim 2, and the specification.

Turning to the objection to the specification on page 3 of the Office Action, note the statement referred to on page 4 of the original specification, reciting that the cards are "...having a thickness of less than about ¼ inch, or less than 0.05 inch". This represents two alternatives, and is not a range as the examiner proposes. The statement is entirely clear. First, it states that the thickness may be "less than about ¼ inch". Then, a narrower scope of disclosure is provided, namely "...less than 0.05 inch" in the nature of a preferred, narrower disclosure.

It is submitted that there is nothing unclear about this disclosure.

Turning to the rejection of claims 21-23 under 35 U.S.C. 112, first paragraph, on page 4 of the Office Action:

The examiner states: "The specification does not describe the creation of authenticator(s) in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

Note the claim chart at the end of this document, where support for claims 21-23 is listed.

The attention of the examiner is directed to page 2 of the specification, where the concept of an authenticator is found. Note the language beginning at line 22:

> "Accordingly, it would be useful to provide a system for biometric identification or identity verification (authentication), which permits a user to effectively maintain possession and control of his or her biometric information.
>
> Systems which store reference biometric data in a central computer or other central repository necessarily require access to such reference data for performing a verification or authentication or identification. . . ." (emphasis added)

Accordingly, it can be seen that the term "authentication" in this application relates to "biometric identification or identity verification". The term "authentication" is a synonym for "verification" or "identification" as shown in lines 27 and 28 of page 2 (see above). Thus an "authenticator" is a device that verifies or identifies.

Turning to page 3, line 9 *et seq.*, of the specification, it is stated: "Accordingly, it would be useful to provide a (preferably lightweight, portable and low cost) biometric identification or authentication system in which the cost of bandwidth and delay associated with the central storage of biometric data on a computer or similar system can be reduced or eliminated." (emphasis added).

Thus, it is clear that the specification teaches an "authentication system" which is lightweight, portable, and of low cost, like a credit or debit card, which called subsequently in the specification a "BDSD", for "portable biometric data storage device" (page 3, lines 16-19). That also can be an "authenticator".

From this, it is clear that the biometric data storage device (BDSD) is related to the term "authentication system" of line 10 of page 3. Accordingly, as taught at page 3, line 22 et seq: "In this manner, when a player wishes to employ the BDSD (carrying a first authenticator) for placing a wager or other gaming purposes, appropriately

configured gaming terminals can obtain (measure) biometric data of the person attempting to use the BDSD and can compare such data with the previously-stored biometric data of the authorized user of the BDSD". (First parentheses added.)

Such a system for measuring the biometric data of a person is certainly part of a "biometric identification or authentication system" as discussed at page 3, line 10. It is also a "system for biometric identification or identity verification (authentication), which permits a user to effectively maintain possession and control of his or her biometric information", as stated at page 2, lines 23-25.

Such information can clearly comprise "...at least one more authenticator in the form of biometric data," as called for in claim 21, step (b).

Turning to step (a) of claim 21, another kind of authenticator from that of step (b) is clearly taught in the specification at page 5, lines 1-6 and page 6, lines 1-4 thereof. This other kind of authenticator is not the biometric authenticator of claim 21(b), but is a "first authenticator" referred to particularly in line 3 of page 5, i.e. "personal and/or financial information 220 relative to the prospective player". As stated, it can include the name, address, social security number, or tax identification number, and the like.

This is clearly another kind of "authenticator", optionally included along with the biometric reference data 218, and clearly supporting step (a) of claim 21.

Accordingly, it is submitted that steps (a) and (b) of claim 21 are disclosed in the specification.

Turning to step (c) of claim 21, note, beginning at line 29 of page 4:

> "When a prospective player approaches a registration desk 112 and requests a BDSD 212, if the prospective player has not already established an account, account establishment will be initiated 214. The registration entity will perform a number of steps including, in the depicted

> embodiment, acquiring biometric reference stated 218 and at least, in least some embodiments, obtaining personal and/or financial information 220 relative to the prospective player. The personal and financial information can include information such as name, address, social security or tax identification number . . . "

It is submitted that this is a clear disclosure of the step of claim 21, step (c). Both the first authenticator, which is data such as social security or tax I.D. number, and the "at least one more authenticator in the form of biometric data", is clearly associated with a player, as claim 21(c) calls for.

Turning then to claim 21, paragraph (d), as stated at page 3, line 22 et. seq:

> "In this manner, when a player wishes to employ the BDSD for placing a wager or other gaming purposes, appropriately configured gaming terminals can obtain (measure) biometric data of the person attempting to use the BDSD and can compare such data with the previously-stored biometric data of the authorized user of the BDSD." (Emphasis added).

The BDSD is clearly supported as carrying a "first authenticator" by the use of the word "authentication" with respect to it in the specification, as discussed above. See page 3, lines 9-12, for example. Player identification is provided by the use of the BDSD and previously-stored biometric data of the authorized user of the BDSD. This is done using the first authenticator (other than biometric data) and the "at least one more authenticator", which comprises the biometric data of the person, as described by the specification in the section quoted above. Furthermore, the two authenticators are stored on a data storage device (BDSD) as disclosed in the specification, as called for in the last line of claim 21.

A chart, showing claims 21-23, and portions of the specification which support said claim, is found at the end of this document, and provides further details of support of the claims.

It is believed that claim 21, and claim 22, are supported by the specification of this application, in the manner discussed above, the similar details of the support being as provided in the enclosed chart.

As such, it is believed that claims 21 and 22 comply both with the enablement requirement of 35 U.S.C. 112, and also the written description requirement of 35 U.S.C. 112.

In Sections 7 and 8 of the last Office Action, the examiner states that claim 23 recites the limitation "electronic transfer", and that this fails to comply with both the enablement requirement and the written description requirement of 35 U.S.C. 112, first paragraph. Claim 23 also uses the term "authenticator", having meaning and support as described above.

Dealing first with support for the phrase "electronic transfer": in Section (d) of claim 23, the step is provided of "recognizing a player request for an electronic transfer." This is accomplished when the player inserts the BDSD into slot 124, causing the BDSD to be read, as called for in particularly the last paragraph of page 6. As stated beginning at specification page 6, line 21: "In response to receipt of the BDSD 118, the gaming terminal 122 actuates an authorization system or subroutine 232. In this configuration, the gaming terminal 122 includes not only a smart card reader (or other device for reading the biometric reference data from the BDSD) but also includes electronic data processing capabilities..."

This certainly comprises the step of "recognizing a player request for an electronic transfer" as called for in claim 23, step (d). The reading of the biometric

reference data from a data storage device comprises, to anyone skilled in the art, a clear instance of electronic transfer.

Step (d) is thus supported at specification page 6, lines 9-11 and 20-30, etc.

In step (e) of claim 23, the step of acknowledging a desired electronic transfer is clearly found in the response of the machine beginning on specification page 6, last line: "Accordingly, the player is prompted to place his or her figure or thumb on the scanner 126 for appropriate biometric measurements . . . in order to allow the terminal to acquire the appropriate biometric data 234. The data measured at the terminal 122 is then compared 236 to (decrypted) reference data from the BDSD 118". (emphasis added).

The stated prompting is a clear acknowledgement.

Continuing on, in claim 23, step (f), the step is "...using said second authenticator to confirm and authorize said desired electronic transfer". This is clearly found in the disclosure beginning on page 7, line 2: "The data measured at the terminal 122 is then compared 236 to (decrypted) reference data from the BDSD 118. "If there is a match, 238, the terminal 122 microprocessor outputs an authorization allowing the player to access his or her account and/or to use the debit card balance 242. If there is no match, the microprocessor 122 may output a notification 244, e.g., to casino personnel to investigate possible use of a lost or stolen BDSD...".

Accordingly, it is believed that claim 23 also complies with both the enablement requirement and the written description requirement of 35 U.S.C. 112, first paragraph.

If the examiner wishes, language of claims 21-23 can be added to the specification, when the examiner has acknowledged that the specification basically includes sufficient disclosure to support claims 21-23.

The examiner has rejected claims 1, 6, 8 and 11-13 as unpatentable over Schneier et al. U.S. Patent No. 6,099,408, in view of Sehr U.S. Publication No. 2001/0018660. Schneier et al. relates to a method and apparatus for securing electronic games. However, Schneier et al. fails to disclose the concept of claim 1, for example, of a biometric data storage device which comprises a debit card. Instead, as taught in Schneier et al., column 4, lines 47-60, data is stored in data storage device 250, which can include various data relating to the player, included in database 255. A biometric device 355 may be added for increased security (column 6, lines 46-47) but it also is not a debit card. Also as shown in column 16, line 6 *et seq.* the player database 255 has biometric information stored in it, and biometric information is obtained from the player for comparison and authentication.

This does not include the concept of storing the biometric information on a debit card, which is carried by the player, so that biometric data concerning the player remains private, and is not stored in the database of a machine.

The Sehr publication teaches a ticketing system, as described in the Abstract, where portable ticketing cards may be smart credit or debit cards, and which may carry biometric identification of the card holders. However, the electronic ticketing system is basically a system providing access to an athletic event, entertainment event, or the like, which is a very different function from the gaming apparatus of this invention.

It is submitted that those skilled in the art, having Sehr and Schneier et al. before them would not be led to the concept of using a debit card of the type which is primarily an admission center entry card, in the field of activation of a gaming machine, which is something entirely different.

Furthermore, note claims 27 and 28, in which the debit card is credited with the player's winnings from play of the gaming apparatus. It is not seen that there is any analog to the function of claims 27 and 28 in either Sehr or Schneier et al. You don't expect money coming back to the card at an athletic event!

Accordingly, it is submitted that claim 1 and its dependent claims are patentable.

Turning to independent claim 8 and its dependent claims, here also, the same distinctions arise relative to the two prior art references combined by the examiner in the rejection concerning this claim.

Claim 8 covers a gaming method, something which is not contemplated at all in Sehr. It is submitted, for the reasons discussed above, that those having Schneier et al. and Sehr before them would not be led to a method for gaming which comprises a card having stored biometric data for authentication and identification. Also, claim 28 adds to the method of claim 8 the crediting of player's winnings to a current account balance carried on the credit card. It is not seen that such crediting of prizes or winnings is taught in Sehr or Schneier et al., and thus such disclosure is not found in the combination.

Accordingly, it is submitted that claim 8 and its dependent method claims are patentable over the rejection.

Referring to independent claim 15, the examiner has rejected it and numerous other claims as unpatentable over Schneier et al. in view of Sehr, further in view of Thompson U.S. Patent No. 5,865,470.

Claim 15 calls for a gaming apparatus comprising a card for storing first biometric data for at least a first user, and also in which the card stores the current account balance for an account established for the user. As before, the gaming terminal and reader is provided, plus a biometric data measuring device and a comparison device for comparing measured biometric data of the player to the first biometric data stored on the card.

As before, Schneier stores its biometric data in an electronic database 255 of a data storage device 250, which is by no means a card. Sehr, on the other hand, uses a smart credit or debit card, but there is no teaching of the use of the card with the gaming apparatus. Sehr, of course, relates to admission to an Event, rather than the playing of a gaming apparatus. It is submitted that the combination rejection proposed by the examiner between Schneier et al. and Sehr is clearly a matter of hindsight, inspired by the disclosures of this application, and that there is nothing in the two documents themselves that would render obvious the limitations of Claim 15.

All that Thompson Patent No. 5,865,470 adds to this latter rejection is a disclosure at Column 4, Lines 45-49: "Conventional plastic credit cards are 0.021 to 0.027 inches in thickness." This fails to add to the rejection the critical, missing element discussed above.

Furthermore, claim 29 calls for the player's winnings upon play of the gaming apparatus to be credited to the current account balance. It is further submitted that

there is no teaching of this crediting of winnings to the current account balance in the teachings of the cited prior art:

In view of the above, allowance of the claims is respectfully requested.

Respectfully submitted,

SEYFARTH SHAW LLP

Garrettson Ellis
Registration No. 22,792
Attorney for Applicant

SEYFARTH SHAW LLP
55 East Monroe Street, Suite 4200
Chicago, Illinois 60603
(312) 269-8567

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Mail Stop: Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Oct 15, 2004.

Registered Attorney for Applicant
Date: Oct 15, 2004

Specification Support for Claims 21-23

21. A method for creating a player identification usable in a gaming environment and having at least two authenticators, the method comprising:	Page 1, 2d paragraph Page 6, lines 1-4
(a) creating a first authenticator;	Page 5, lines 1-6 Page 6, lines 1-4
(b) entering at least one more authenticator in the form of biometric data;	Page 3, lines 16-25 Page 5, lines 1-2 and 11-16
(c) associating said first authenticator and said at least one more authenticator with a player;	Page 4, line 29 – Page 5, line 6
(d) providing player identification at a game device having an associated biometric reader using said first authenticator and at least one of said at least one more authenticators, where said first authenticator is a data storage device.	Page 6, lines 1-4; line 25 to page 6, line 8 Page 3, lines 22-25 Page 10, lines 14-18 Page 12, lines 1-3
22. A method for creating a player identification usable in a gaming environment and having at least two authenticators, the method comprising:	Page 1, 2d paragraph Page 6, lines 1-4
(a) creating a first authenticator;	Page 5, lines 1-6 Page 6, lines 1-4
(b) entering at least one more authenticator in the form of biometric data;	Page 3, lines 16-25 Page 5, lines 1-6
(c) associating said first authenticator and said at least one more authenticator with a player and further identifying said first authenticator as an authenticator that will be the authenticator used for searching and identifying said player in a player identification database; and	Page 4, line 29- page 5, line 6 Page 10, lines 14-18

(d) providing player identification at a game device having an associated biometric reader using said first authenticator and at least one of said at least one more authenticators.	Page 6, lines 1-4; line 25 to page 6, line 8 Page 3, lines 22-25 Page 10, lines 14-18 Page 12, lines 1-3
23. A method for enabling electronic transfers using at least two authenticators where any authenticator that is not the first authenticator uses biometric data, in a gaming environment while using a game device having an associated biometric reader, the method comprising:	Page 5, lines 1-6 and 17-28 Page 6, lines 1-4 and 9-11 and 20- page 7, line 8
(a) having a first authenticator readable by a reader associated with said game device;	Page 6, lines 1-4 and 20-25 Page 5, lines 1-6
(b) having a second authenticator different from said first authenticator and readable by a reader associated with said game device;	Page 5, lines 1-6; 11-14 Page 3, lines 16-25
(c) having an entry in a player identification database, where said entry further comprises first authenticator data and second authenticator data;	Page 6, lines 1-4
(d) uniquely associating a player using a game device with an entry in said player identification database and recognizing a player request for an electronic transfer;	Page 6, lines 9-11 and 20 – page 7, line 8
(e) acknowledging a desired electronic transfer;	Page 6, lines 9-11 Page 6, line 29 – page 7, line 2
(f) using said second authenticator to confirm and authorize said desired electronic transfer.	Page 7, lines 2-5